



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/976,471	10/11/2001	James L. Jason JR.	10559-504001 / P11796	9923
20985 7590 03/29/2007 FISH & RICHARDSON, PC P.O. BOX 1022 MINNEAPOLIS, MN 55440-1022			EXAMINER DIVECHA, KAMAL B	
			ART UNIT 2151	PAPER NUMBER
SHORTENED STATUTORY PERIOD OF RESPONSE 3 MONTHS		MAIL DATE 03/29/2007	DELIVERY MODE PAPER	

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary

Application No.

09/976,471

Applicant(s)

JASON ET AL.

Examiner

KAMAL B. DIVECHA

Art Unit

2151

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 February 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-46 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-46 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☒ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

DETAILED ACTION

Claims 1-46 are pending in this application.

Claims 4-5, 8, 15-18, 22, 25-26, 36, 38, 40, 42, 44-46 are cancelled.

Response to Arguments

Applicant's arguments filed January 22, 2007 in a Request for Continued Examination (RCE) have been fully considered but they are not persuasive.

In response filed, applicant argues in substance that:

a. The amended Independent claims include, among other features, generating one or more items of tuple cache information for request messages of a specified type (e.g. SYN request) and determining the number of valid request messages by analyzing the one or more items of tuple cache information. These features are not disclosed by Chen et al. (Remarks, page 10).

In response to argument [a], Examiner respectfully disagrees.

Independent claim 1 recites:

A method comprising:
first monitoring network traffic, and generating one or more items of tuple cache information for request messages of a specified type;
determining a number of valid request messages by analyzing the one or more items of tuple cache information;
comparing current network traffic to the number of valid request messages, at first and second points of a network, and using said comparing to generate information about unwanted communications passing through the first and second points, the unwanted communications being of a type to reduce the ability of the target device to respond to other communications;
communicating the information generated about the unwanted communications to brokers corresponding to the first and second points of the network;
analyzing, by the brokers, the information generated about the unwanted communications; and
communicating between the brokers to identify which of the points first carried the unwanted communications.

Art Unit: 2151

A portion of the applicant's disclosure that supports one or more limitations of the claim above has been reproduced (specification, page 6 line 23 to page 7 line19):

"In detecting a flood attack, a flood detector may employ one or more of the several detection methods...Still another example of flood detection method is comparing or correlating the number of SYN requests with corresponding final ACK messages in order to determine the number of SYN requests that are valid or invalid. A 5-tuple caching technique can be used to handle packets that have been already been seen. When the first SYN message comes in, the cache won't have an entry for the 5-tuple of that message (source IP, destination IP, IP protocol, source port, and destination port). When subsequent packets arrive, there will already be cached information".

In view of the disclosure above, the tuple cache information can be any one of the source IP, destination IP, IP protocol, source port, and destination port.

Chen et al. (Prior Art).

Chen, from the similar problem solving area, discloses a distributed system, comprising plurality of data collectors and gateways in communication with the control center for protecting against DoS attacks via intelligent traffic analysis and filtering (pg. 2 [0025]-[0027]).

A plurality of gateways are deployed at corresponding plurality of locations, and these gateways includes a monitoring process that monitors traffic that passes through the gateway as well as a communication process that can communicate statistics collected in the gateway with the data center and/or control center (pg. 2 [0031]).

Data collectors can be dispersed throughout the network and/or can be strategically disposed at peering points or points of presence, i.e. at first and second points of a network. These data collectors monitor and collect information pertaining to network traffic flow. The data collectors process statistics based on monitored network traffic. Data collectors include a monitoring process, as well as communication process that communicate with data center and/or control center (pg. 3 [0035]).

The data collectors samples one packet in every (n) packets and has counters to collect statistics about every packet. The data collectors parses information in the sampled packet. Information collected includes source information, which may be fake or spoofed (pg. 3 [0037]) such as source IP address.

Stated another way, data collectors monitors and generates the item(s) of tuple cache information for request messages of a specified type in a log (see also, pg. 6 [0078-0079]: source IP, destination IP, protocol, etc.).

Additionally, the data collectors maintains a log that specifies that the data collectors has seen a certain number of packets of a particular kind, that originated from a particular source to a particular destination (pg. 3 [0037]).

Note: in order to detect that the particular kind of packet originated from a particular source, the data collector needs to parse the packet and analyze the source information such as IP address.

Based on the rules within the data collectors, the data a collector analyzes the collected statistics, i.e. collected tuple cache information, and may if necessary compose a message that raises an alarm (pg. 3 [0038]). For example: the data collector may raise an alarm if the incoming packet is associated with an attack.

The fact that “data collector maintains a log of information including number of packets of a particular kind, originated from a particular source to a particular destination” and “analyzes the collected statistics, i.e. tuple information, against the rules” logically implies the presence of determination of a number of valid request messages by analyzing tuple cache information such as source and/or destination information.

Art Unit: 2151

The control center receives information from one or more gateways and data collectors and performs appropriate analysis using an analysis process (pg. 3 [0039]).

Furthermore, the control center communicates with gateways and data collectors in order to identify the attacking networks (pg. 4 [0045-0049]). Stated another way, the control center communicates with gateways and data collectors to identify which of the points first carried information.

Therefore, applicant argument directed towards the distinction between the prior art and the claimed invention based on the features above are considered not persuasive.

Art Unit: 2151

Specification

The specification is objected to under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

The test to be applied under the written description portion of 35 U.S.C. § 112, first paragraph, is whether the disclosure of the application as originally filed reasonably conveys to the artisan that the inventor had possession at that time of later claimed subject matter. Vas-Cat, Inc. v. Mahurkar, 935 F.2d 1555, 1565, 19 USPQ2d 111, 1118 (Fed. Cir. 1991), reh'rg denied (Fed. Cir. July 8, 1991) and reh'rg, en banc, denied (Fed. Cir. July 29, 1991).

The applicants have failed to provide an enabling disclosure in the detailed description of the embodiment. The specification is objected to under 35 U.S.C. § 112, first paragraph, as failing to support the subject matter set forth in these claims, i.e. lack of written description. See MPEP § 2163.

Independent claim 1 recites:

A method comprising:
first monitoring network traffic, and generating one or more items of tuple cache information for request messages of a specified type;
determining a number of valid request messages by analyzing the one or more items of tuple cache information;
comparing current network traffic to the number of valid request messages, at first and second points of a network, and using said comparing to generate information about unwanted communications passing through the first and second points, the unwanted communications being of a type to reduce the ability of the target device to respond to other communications;
communicating the information generated about the unwanted communications to brokers corresponding to the first and second points of the network;
analyzing, by the brokers, the information generated about the unwanted communications; and
communicating between the brokers to identify which of the points first carried the unwanted communications.

Art Unit: 2151

However, upon reviewing the originally filed specification, Examiner noted that there is no support for the amendatory claim language and/or limitations in the original specification.

In other words, the originally filed specification fails to teach, disclose or suggest the process of “comparing current network traffic to the number of valid request messages, at first and second points of a network...”

As such, the above claimed limitations presents the subject matter situations and was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

1. Claims 1-3, 6-7, 9-14, 19-21, 23-24, 27-35, 37, 39, 41 and 43 are rejected under 35

U.S.C. 112, first paragraph, for the same reasons as set forth in specification above.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 1-3, 6-7, 9-14, 19-21, 23-24, 27-35, 37, 39, 41 and 43 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 1 recites “tuple cache information” in the claim.

In the context of this claim, it is unclear what type of information the term is referring to.

Applicant is advised to clearly define the term in the context of the claims.

Additionally, in the context of the claims it is unclear whether the process of monitoring network traffic, determining a number of valid request messages, comparing, communicating, etc., is with respect to brokers or the device associated with first and second points of a network.

Claim 1 also recites “...comparing current network traffic to the number of valid request messages, at first and second points of a network, and using said comparing to generate information about unwanted communications passing through the first and second points...”

It is unclear how this process is achieved. In other words, how does the process of comparing current network traffic, i.e. incoming packet, to the number of valid request messages (i.e. a number and/or threshold) generates the information about unwanted communication is achieved.

Claims 2-3, 6-7, 9-14, 19-21, 23-24, 27-35, 37, 39, 41 and 43 are rejected for the same reasons as set forth in claim 1.

For examination purposes, the tuple cache information will be interpreted as information related to communication.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claims 31-35, 37, 39, 41 and 43 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 31 recites:

“A computer program embodied in a computer readable medium...”

First, based on the context of the claim, the claim fails to fall into any of the four enumerated categories of the statutory subject matter, as set forth above.

Secondly, the claim lacks an appropriate computer readable storage medium to define a structural and functional interrelationship between a computer program and other elements of a computer, which permit the functionality of the computer program to be realized.

The applicant specification is evidenced to disclose computer readable medium to include both tangible medium such as such as memory chips, magnetic media, optical media and intangible medium such as those delivered for execution electronically from a remote location, i.e. through transmission media.

The transmission media is incapable of producing useful, concrete (repeatable) and tangible results.

For the at least these reasons, the claim is considered non-statutory.

Claims 32-35, 37, 39, 41 and 43 are rejected for the same reasons as set forth in claim 31.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-3, 6-7, 9-14, 19-21, 23-24, 27-35, 37, 39, 41 and 43 are rejected under 35

U.S.C. 102(e) as anticipated by Chen et al. (hereinafter Chen, US 2002/0103916 A1).

As per claim 1, Chen explicitly discloses a method comprising:

first monitoring network traffic, and generating one or more items of tuple cache information for request messages of a specified type (pg. 1 [0007-0008], pg. 2 [0027], pg. 3 [0035-0039], pg. 6 [0078-0079], fig. 6 item #32a, fig. 4 item #42, 44);

determining a number of valid request messages by analyzing the one or more items of tuple cache information (pg. 3 [0035-0039], pg. 4 [0045-0048]: log of information including number of packets seen by the data collector of certain type from a particular source);

comparing current network traffic to the number of valid request messages, at first and second points of a network, and using said comparing to generate information about unwanted communications passing through the first and second points, the unwanted communications being of a type to reduce the ability of the target device to respond to other communications (pg. 1 [0006-0007], [0009], pg. 4 [0048-0052], pg. 5 [0059-0062], fig. 9 item #84, 86, 88, 89 and 90);

communicating the information generated about the unwanted communications to brokers corresponding to the first and second points of the network (pg. 4 [0045-0048]: communicating statistics or alert to the control center and/or data collector);

analyzing, by the brokers, the information generated about the unwanted communications (pg. 4 [0045-0048]);

communicating between the brokers to identify which of the points first carried the unwanted communications (fig. 4 item #46, 50, 52, fig. 6, fig. 9, pg. 2 [0027-0028], pg. 3 [0035-0038], pg. 4 [0045-0050]: communicating with control center and data collectors and gateways to identify and trace the source of the attack).

As per claim 2, Chen discloses the process of detecting the direction of the unwanted communications (pg. 3 [0037]).

As per claim 3, Chen discloses the process of identifying the target device (pg. 3 [0037]).

As per claim 6, Chen discloses the process of correlating communications request messages with acknowledgement messages (pg. 1 [0006-0009], pg. 3 [0035], [0037]).

As per claim 7, Chen discloses the process of communicating information about the unwanted communications to brokers (pg. 1 [0007, 0009], pg. 2-3 [0031]).

As per claim 9, Chen discloses the process of blocking a portion of communications passing through the point through which the unwanted communications originated (pg. 2 [0028], pg. 2-3 [0031], pg. 4 [0043]).

As per claim 10, Chen discloses the process of blocking a portion of communication request messages passing through the point through which the unwanted communications originated (pg. 2-3 [0003], pg. 4 [0043], [0047]).

As per claim 11, Chen discloses the process wherein the target device comprises a web server (pg. 2 [0025], pg. 5 [0060], fig. 2-3).

As per claim 21, Chen discloses the system wherein the communications analyzer includes an interface monitor corresponding to each interface device and a communications link between the interface monitors (pg. 2-3 [0030-0031], fig. 1-3).

As per claim 27, Chen discloses the process in which the communications monitor also includes a statistics analyzer for statistically analyzing the messages passing through the plurality of agents (pg. 3 [0035], fig. 4 item #44, 50, fig. 6, fig. 9).

As per claim 35, Chen discloses the process wherein said network traffic of a specified type is a number of SYN requests (pg. 1 [0006-0011], fig. 4, fig. 10).

As per claims 12-14, 19-20, 23-24, 28-32, 37, 39, 41 and 43, they do not teach or further define over the limitations in claims 1-3, 6-7, 9-11, 21, 27 and 35. Therefore claims 12-14, 19-20, 23-24, 28-32, 37, 39, 41 and 43 are rejected for the same reasons as set forth in claims 1-3, 6-7, 9-11, 21, 27 and 35.

Additional References

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- a. Sharp et al., US 2002/0131366 A1: Traffic Management Control.
- b. Belissent, US 6,789,203 B1: Preventing DoS Attack.
- c. Conklin et al., US 5,991,881: Network Surveillance system.

Art Unit: 2151

Conclusion

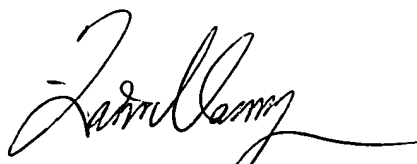
Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAMAL B. DIVECHA whose telephone number is 571-272-5863. The examiner can normally be reached on Increased Flex Work Schedule.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Zarni Maung can be reached on 571-272-3939. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Kamal Divecha
Art Unit 2151
March 20, 2007.



ZARNI MAUNG
SUPERVISORY PATENT EXAMINER